REMARKS

Claims 1 – 12 are now pending in the application. Applicant respectfully requests that the Examiner reconsider and withdraw the rejection(s) in view of the following remarks.

REJECTION UNDER 35 U.S.C. § 103

The Examiner rejected claims 1 – 12 under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art (AAPA) in view of Caputo et al. (U.S. Pat. No. 5,778,071). Applicant respectfully traverses this rejection.

The invention is directed to a clear text transmission security method. Transaction terminals having PIN entry devices typically have keypads for entering data into the PIN device and displays for displaying messages to the user of the PIN devices, including prompting the user to enter data. This data is often transmitted to remote devices. Sensitive data, such as credit card numbers and PIN numbers, is encrypted before it is sent to the remote devices. However, to reduce overhead, some transaction terminals transmit non-sensitive data, such as odometer readings, in clear text form, that is, without encrypting it. Since this data is entered into the PIN transaction terminal by the user in response to a prompt, the PED Spec. (see page 3 of the Application) requires that data entered into a PIN entry device can be transmitted to the remote device as "clear text" data only if it was input in response to a secure prompt. As defined in the application, a "secure prompt" is a prompt that prompts for entry of non-sensitive data. [Application, p. 4] To comply with the PED Spec. requirements, the PIN devices have included a table of secure prompts stored in the PIN devices' memories. The PIN device then compares the prompt received from the remote device with the table of secure prompts and transmits data entered

into it in clear text form only if the data entry prompt from the remote device matches one of the secure prompts in the table.

Prior to applicant's invention, the prompt received from the remote device had to match exactly an entry in the table of secure prompts stored in the PIN's memory. Since remote devices made by different manufacturers often use somewhat different prompts to prompt for the entry of the same information, each variation of a secure prompt had to be stored in the secure prompt table.

Applicant's invention solved the problem of having to store multiple variations of secure prompts for the entry of the same data. In an illustrative embodiment, applicant's invention determines that a prompt received from a remote controller is a secure prompt not only when it matches exactly a prompt stored in the secure prompt table, but if it matches only a portion of any prompt in the secure prompt table, or any prompt in the secure prompt table matches any portion of the received prompt. Doing so reduces the amount of memory needed for the secured prompt table.

Claims 1, 2, 4, 6, 8 and 10 and 12 are the independent claims. Turning first to claim 1, claim 1 is directed to a security method for transmission to a remote device of data input into a transaction terminal as clear text data. As discussed above, transmission of data as clear text data is transmitting the data without encrypting it. Claim 1 recites, in pertinent part:

"determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i) the data entry prompt matching at least one of the prompts in the secure prompt table,

(ii) the data entry prompt matching only a portion of any of the secure prompts in the secure prompts table, and

(iii) any of the prompts in the secure prompt table matching only a portion of the data entry prompt.

The Examiner concedes that the AAPA does not disclose these limitations. But the Examiner takes the position that Caputo discloses "a digital algorithm (algorithm or plain text data) that includes a private/public keys or portion of the secure prompts."

Applicant submits that Caputo fails to disclose the above limitations of claim 1. Caputo is directed to a portable security device that can be carried by an individual and connected to telephone circuits to both authenticate the individual and encrypt data communications. [Caputo, Abstract] Caputo does not disclose or discuss the transmission of data as clear text data, and in particular, any security method where data is transmitted as clear text data only in response to a secure prompt. In contrast, Caputo's data is encrypted before it transmitted, as can be seen from the first section of Caputo cited by the Examiner. "Nonetheless, referring again to Fig. 6, **plain text data 72 (i.e., non-encrypted data) is encrypted** (Block 74) using one or more of a plurality of encryption algorithms well know to practioners . . . ." [Caputo, col. 10, lines 61 – 64 (emphasis added)] The second section of Caputo cited by the Examiner deals with the sender of the encrypted data authenticating it and the receiver verifying it, as can be seen by the discussion in Caputo that introduces the second section cited by the Examiner. [See, Caputo, col. 12, lines 14 – 17]. But a sender authenticating encrypted data and the receiver verifying it does not involve a method for transmitting data in clear text form in response to a secure data prompt. The third section of Caputo cited by the Examiner deals with device and user authentication, i.e., digital signatures, as can be seen from the section of Caputo introducing the third section cited by the Examiner.

[See, Caputo, col. 14, lines 10 - 14]. This again does not deal with transmitting data in clear text form in response to a secure data prompt. Applicant submits that claim 1 is thus allowable over the combination of the AAPA and Caputo.

Claim 2 recites, in pertinent part:

> determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching any prompt in the secure prompt table, and
>
> (ii) any prompt in the secure prompt table matching only a portion of the data entry prompt.

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo. As discussed, Caputo does not disclose or discuss the transmission of data as clear text data, and in particular, any security method where data is transmitted as clear text data only in response to a secure prompt. Applicant submits that claim 2 is thus allowable over the combination of the AAPA and Caputo.

Claim 4 recites, in pertinent part:

> determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:
>
> (i) the data entry prompt matching any prompt in the secure prompt table, and
>
> (ii) any prompt in the secure prompt table matching only a portion of the data entry prompt.

Again, the Examiner admitted that the AAPA does not disclose these limitations. Neither does Caputo. As discussed, Caputo does not disclose or discuss the transmission of data as clear text data, and in particular, any security method where

data is transmitted as clear text data only in response to a secure prompt. Applicant submits that claim 4 is thus allowable over the combination of the AAPA and Caputo.

The remaining independent claims, claims 6, 8, 10 and 12, contain limitations comparable to the limitations discussed above with respect to one or more of claims 1, 2 and 4. Applicant submits that claims 6, 8, 10 and 12 are thus allowable over the combination of the AAPA and Caputo.

The dependent claims, claims 3, 5, 7, 9 and 11 depend from respective ones of the independent claims and are allowable for at least that reason.

CONCLUSION

Applicant submits that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: Feb. 16, 2009

By: R A. Fuller III
Roland A. Fuller III, Reg. No. 31,160

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600
RAF/jy